ハッシュ関数

形式化数学研究室
宮島啓一

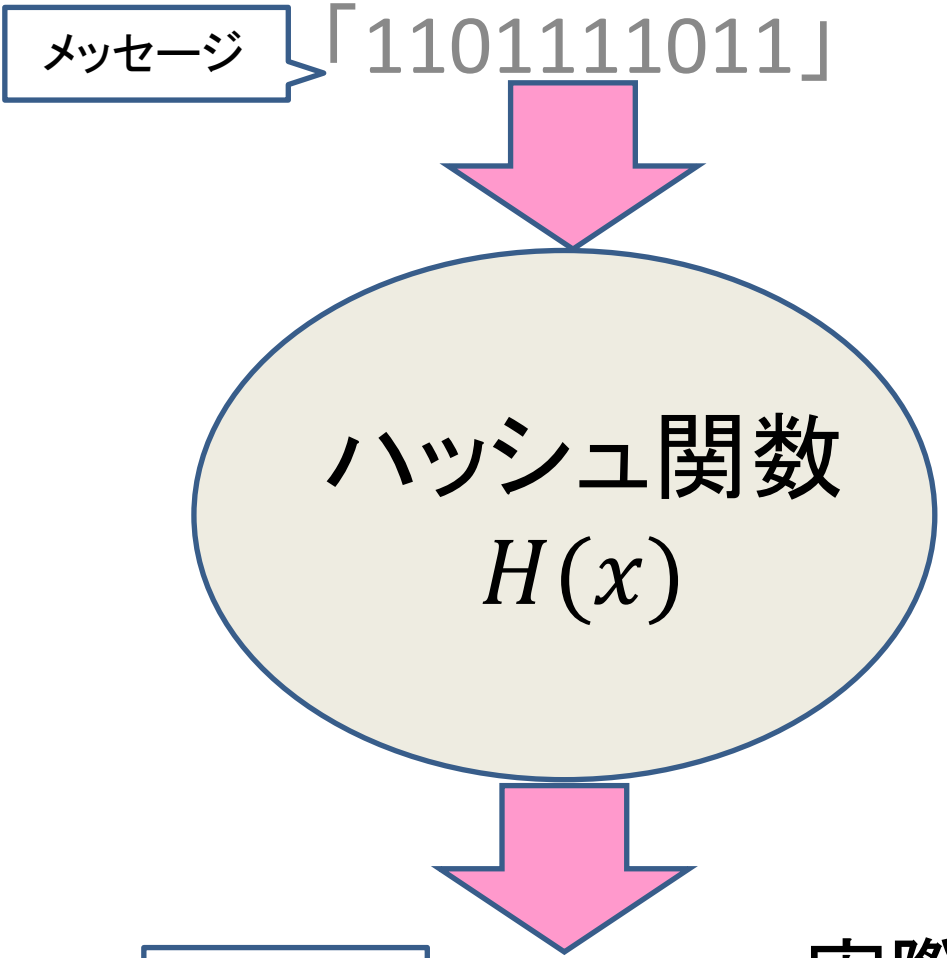
ハッシュ関数とは？

「長いメッセージを短くする関数」
のことである。一般に、

$$H(m)$$

と表す。ここで、m はメッセージである。

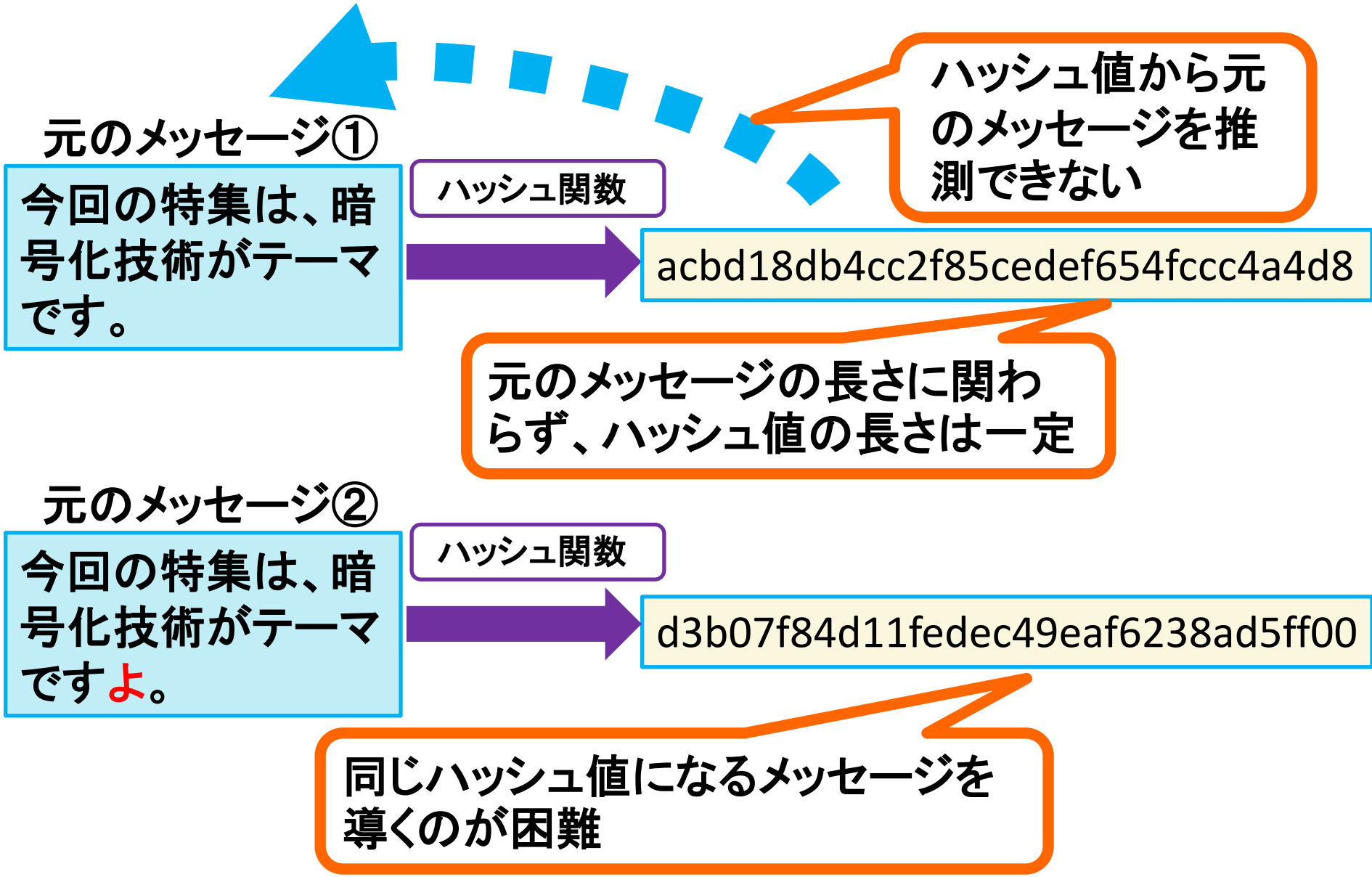
例えば、ハッシュ関数が
「10ビットのメッセージを3ビットに短縮する」
とする。



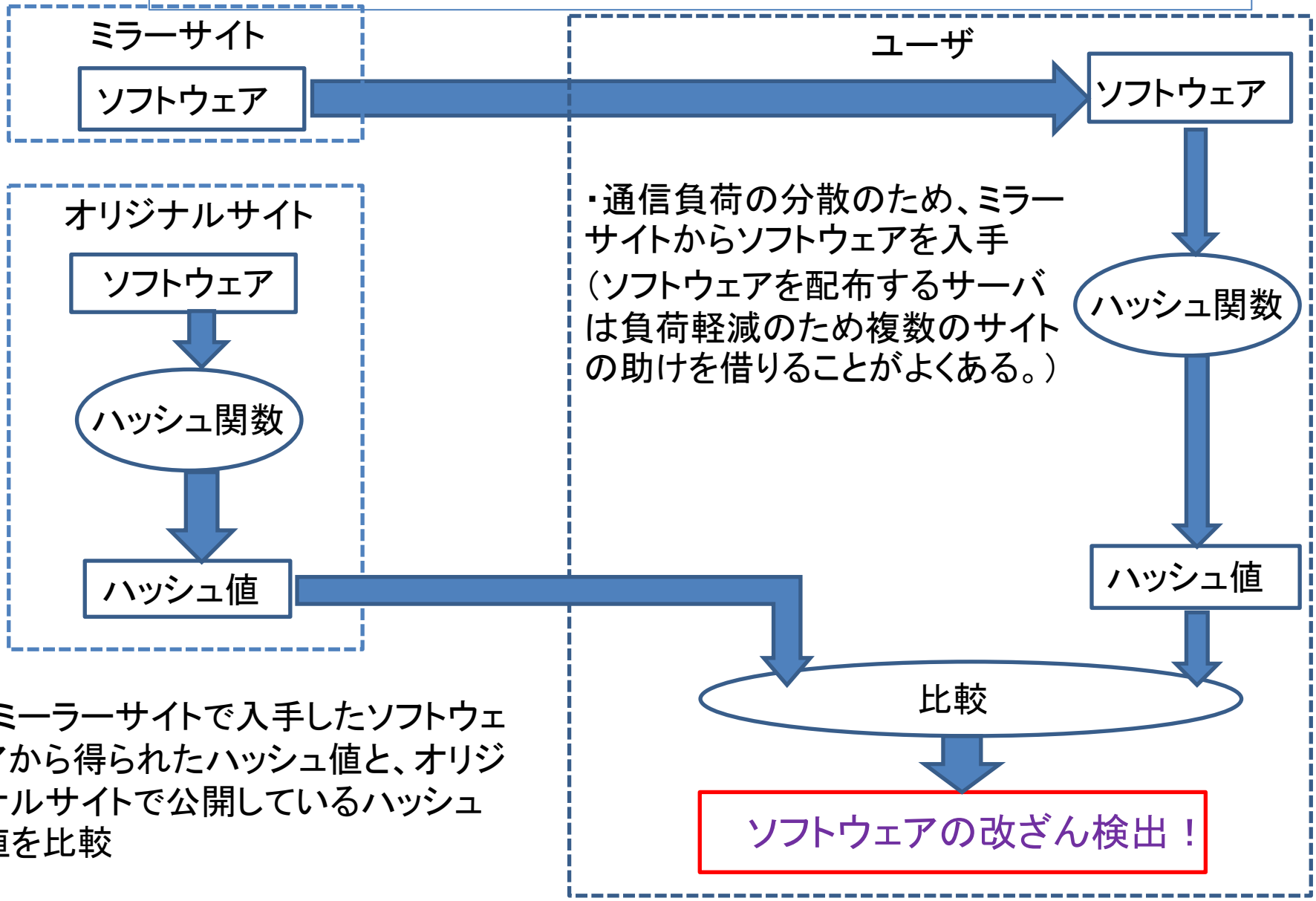
逆向きに「元に戻す」
ことは考えなくてよい

← 実際にはこの部分がもっと長い！

ハッシュの特徴

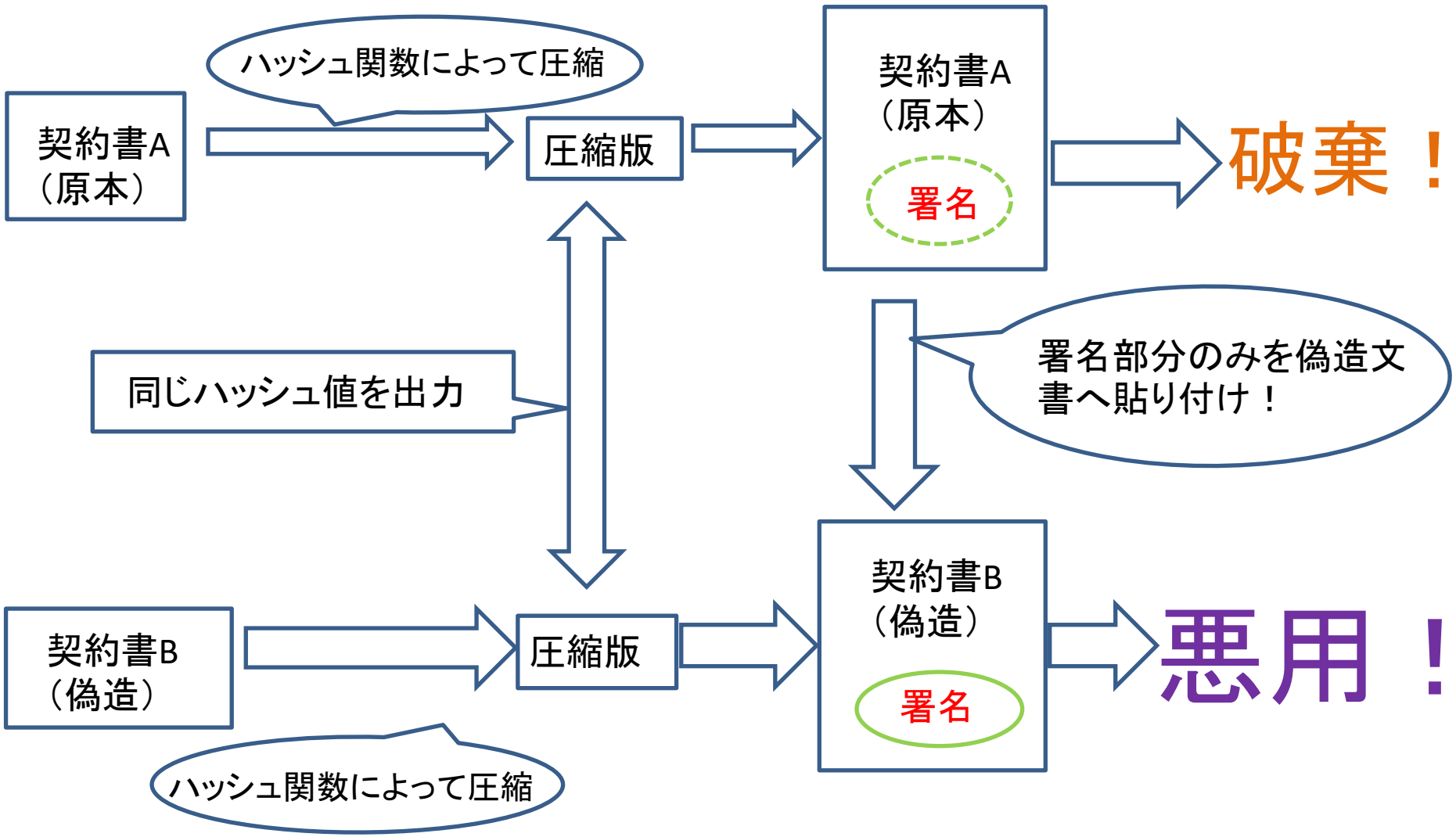

元のメッセージ①
今回の特集は、暗号化技術がテーマです。
ハッシュ関数
acbd18db4cc2f85cedef654fccc4a4d8
ハッシュ値から元のメッセージを推測できない
元のメッセージの長さに関わらず、ハッシュ値の長さは一定
元のメッセージ②
今回の特集は、暗号化技術がテーマですよ。
ハッシュ関数
d3b07f84d11fedec49eaf6238ad5ff00
同じハッシュ値になるメッセージを導くのが困難

～ハッシュ値の衝突による問題点～
（ソフトウェアの改ざん検出の場合）



・ミーラーサイトで入手したソフトウェアから得られたハッシュ値と、オリジナルサイトで公開しているハッシュ値を比較

～ハッシュ値の衝突による問題点～
（デジタル署名の場合）



～ハッシュ関数の脆弱性～

・バースデーパラドックスの理論によると、ハッシュ関数SHA-1の場合、約2^{80}回の計算を行えば、同じハッシュ値を発生するメッセージの組みを少なくとも一つ作り出せる。

～ハッシュ関数の脆弱性～

・SHA-1に対する攻撃法が2005年に発表される。

$$2^{80} \Longrightarrow 2^{69}$$

危険性が2048倍増加！！

→現在に至るまで多くの企業や公的機関がSHA-1を利用した証明書等を受け入れないようにする事を表明

～ハッシュ関数の脆弱性～

・米国国立標準技術研究所（NIST）は合衆国政府組織に対し、2010年までにSHA-2に移行するように要請。

・SHA-2は構造がSHA-1に似ているが、その有効な攻撃法は未だ報告されていない。

ご清聴ありがとうございました

参考文献

- 現代暗号の基礎数理
- 現代暗号への招待
- 暗号技術入門
- 数理的技法による情報セキュリティー